UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
	)	
v.	)	
	)	**DOCKET NO. 16-CR-10305-NMG**
	)	
MARTIN GOTTESFELD	)	

MOTION TO SUPPRESS EVIDENCE

Martin Gottesfeld moves to suppress evidence obtained by the government as a result of their execution of a search warrant for his Somerville apartment on October 1, 2014.[1] The search warrant relied upon information derived from the government's warrantless, constant, real-time and long-term surveillance of Gottesfeld's internet activity. This information was obtained in violation of Gottesfeld's Fourth Amendment rights. Absent this illegally obtained information, the search warrant fails to establish probable cause to believe evidence of a crime would be found in Gottesfeld's apartment and that seizure of all computers and electronic devices in that home was necessary. For these reasons, Gottesfeld seeks to suppress from evidence at trial any items taken from his home during the execution of the search warrant, and any information obtained by the government as a result of the seizure of those items.

BACKGROUND

The government obtained the search warrant for Gottesfeld's apartment after investigating a Distributed Denial of Service ("DDOS") attack on Boston Children's Hospital fundraising webpage on April 20, 2014. In their application for this search warrant, the government sets forth their belief that the DDOS attack was part of an "activist effort concerning the custody battle over teenage

[1] A copy of the search warrant and its application are attached as Exhibit A. All exhibits are filed under seal in accordance with the Protective Order pertaining to discovery in this case. *See* D.E. 43 (Nov. 21, 2016).

medical patient Justina Pelletier." Ex. A. at ¶9. They cite a YouTube video titled "Anonymous #OpJustina Press Release Video" which was posted from a YouTube account belonging to Martin Gottesfeld on March 23, 2014. *Id.* at ¶¶10, 16. This video, which claimed to be from the group Anonymous, stated that Anonymous "will punish all those held accountable and will not relent until Justina is free," ordered Children's Hospital to terminate the employment of one of the doctors involved in Justina Pelletier's treatment, and warned "Test us and you shall fail." *Id.* at ¶¶11, 12. The video concludes with a link to a website that had the address, phone number, website address, and IP address for Boston Children's Hospital. *Id.* at ¶13. Agents learned that the YouTube video was posted using an IP address belonging to Martin Gottesfeld. *Id.* ¶17.

On July 17, 2014, three months after the DDOS attack on Children's Hospital, the government obtained a pen register/trap and trace order from the Court allowing them to collect, in real-time, the IP addresses sending communications to, and receiving communications from, Gottesfeld's IP address for 60 days.[2] The order also allowed the government to obtain the subscriber information associated with each IP address communicating with Gottesfeld's IP address.

From that the order, the government gathered information that showed that Gottesfeld was using a VPN service through the website www.riseup.net, and also that he was using the TOR network. Ex. A. at ¶¶22, 24. The government noted this information in their search warrant application and also noted that two Twitter accounts that had posted about the Children's Hospital DDOS attack used these same services. *Id.* at ¶25. The government also noted that criminals frequently use these types of anonymizing services to mask their criminal activities. *Id.* at ¶26.

The government also learned that Gottesfeld was an outspoken activist against the troubled teen industry and was critical of other institutions that abused and mistreated children residing at

[2] The application for the Pen Register/Trap and Trace Order is attached as Exhibit B. The order is attached as Exhibit C.

their facilities. Ex. A. at ¶¶28-31. Two of those institutions that Gottesfeld was critical of also experienced DDOS attacks. *Id.* at ¶¶39, 31.

On September 29, 2014, the government obtained a search warrant to search Gottesfeld's apartment in Somerville. The warrant authorized them to seize a long list of items, including all computer hardware (including tablets and smart phones), computer software, and storage media. When the police searched Gottesfeld's apartment on October 1, 2014, they took multiple computers, storage media, and Gottesfeld's smart phone. The police later examined those devices and discovered evidence implicating Gottesfeld in the DDOS attack against Children's Hospital.

I. THE WARRANTLESS SURVEILLANCE OF MR. GOTTESFELD'S INTERNET ACTIVITIES WAS UNLAWFUL AND MERITS SUPPRESSION

As part of its investigation, the government requested and obtained an *ex parte* order under the Pen Register/Trap and Trace Statute ("Trap/Trace"), 18 U.S.C. § 3121–27, and the Stored Communications Act ("SCA"), 18 U.S.C. § 2703. The former permitted it to have the Internet Service Provider ("ISP") install a Trap/Trace device that would trace the "source and destination of all electronic communications directed to or originating from" Gottesfeld's IP address and transmit that information to the government, "continuously," in real time, 24 hours a day for 60 days. *See* Ex. B at 1, 5. The latter enabled it to obtain the subscriber information for each IP address Gottesfeld communicated with. *See id.* § 2703(c)&(d). Below, Gottesfeld argues that the order exceeded statutory authority and that the surveillance constituted a search and seizure under the Fourth Amendment. He acknowledges authority to the contrary. Nevertheless, he maintains that the reality of modern technology consumption compels the conclusion that individuals have a reasonable expectation of privacy in their online activities. Furthermore, source and destination information, when aggregated over a long period of time, reveals constitutionally and statutorily protected "content" information. The Supreme Court is poised to revisit the third party doctrine, which has

heretofore insulated this information from Fourth Amendment protection, in *Carpenter v. United States*, S.Ct. No. 16-402 (cert. granted June 5, 2017).

A. THE FOURTH AMENDMENT PROHIBITS THE WARRANTLESS SURVEILLANCE OF AN INDIVIDUAL'S ONLINE ACTIVITY

1. Internet Information Is Protected by the Fourth Amendment Right to Privacy

Since at least 1967, the Supreme Court has recognized that the Fourth Amendment protects an individual's right to privacy, even in public places. *Katz v. United States*, 389 U.S. 347, 351 (1967). *Katz* held that when the government infringes upon a subjective expectation of privacy that society recognizes as reasonable, it effects a search and seizure within the meaning of the Fourth Amendment. *Id.* at 353. Thus, in *Katz*, the government was found to have violated the defendant's Fourth Amendment rights by eavesdropping on his private conversation in a public phone booth. *Id.*

In *United States v. Knotts*, the Court first applied the *Katz* test to electronic surveillance, holding that the Fourth Amendment was not violated when the government used a beeper to track a car. 460 U.S. 276, 277 (1983). The beeper tracking in *Knotts* did not implicate the Fourth Amendment because "[a] person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements…. [By travelling on public streets] he voluntarily conveyed …the fact that he was travelling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination…." *Id.* at 281. However, the Court left open the possibility that advances in surveillance technology would require it to reevaluate its decision. *Id.* at 283-84.

The following year, in *United States v. Karo*, the Court limited *Knotts* to electronic surveillance *in public places*. 468 U.S. 705, 714 (1984). In *Karo*, the police placed a beeper in a container belonging to the defendant and monitored its location electronically, including while it was inside a private residence. *Id.* at 708-10. The Court held that the monitoring of the beeper inside the home was an

unconstitutional trespass into the residence by electronic means. *Id.* at 715; *see also Kyllo v. United States*, 533 U.S. 27, 34 (2001) (Fourth Amendment violated by thermal imaging of a house).

In *United States v. Jones*, five Justices of the Court found that GPS monitoring of a car, in public places, for one month impinged on a legitimate expectation of privacy. 132 S. Ct. 945, 954 (2012); *id.* at 955 (Sotomayor, J., concurring); *id.* at 965 (Alito, J., concurring). In *Jones*, the government placed a GPS tracker on the defendant's car and used it to monitor the car's location – on public thoroughfares – for 28 days. *Id.* at 948. The majority opinion held that the government had violated the Fourth Amendment by the physical trespass of placing the tracker on the vehicle, and it therefore did not need to address whether the location tracking violated a reasonable expectation of privacy. *Id.* at 949. It explicitly noted, however, that "[s]ituations involving merely the transmission of electronic signals without trespass would *remain* subject to *Katz* analysis." *Id.* at 953 (emphasis in original).

The five Justices who did engage in a *Katz* analysis concluded that the government's actions in tracking the car's location violated the Fourth Amendment. *Id.* at 955 (Sotomayor, J., concurring); *id.* at 964 (Alito, Ginsburg, Breyer, & Kagan, JJ., concurring). Justice Sotomayor agreed that prolonged electronic surveillance violates the Fourth Amendment. *Id.* at 955. She added, however, that "even short-term monitoring" raises concerns under *Katz* because "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations." *Id.* She questioned "whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain . . . their political and religious beliefs, sexual habits, and so on." *Id.* at 956 (Sotomayor, J., concurring). And Justice Alito wrote, for four justices, "society's expectation has been that law enforcement agents and others would not . . . secretly monitor and catalogue every single movement of an individual's car for a very long period." *Id.* at 964.

Just as the government catalogued "every single movement" of Jones' car, as it travelled the physical world, the government here has surveilled "every single movement" of Gottesfeld's, as he travelled the internet. Both types of surveillance – GPS tracking of a car and internet tracking of destination IP addresses – reveal the destinations an individual visits, but not the activity s/he partakes in once s/he arrives at a given destination.[3] The surveillance simply sits dormant and waits until the individual leaves and goes to a different destination address. When grafted in small segments, the information revealed by such a search does not trigger the Fourth Amendment. *See Knotts*, 460 U.S. at 281 (no reasonable expectation of privacy in an individual's "movements from one place to another," "on public thoroughfares"). Yet we know from *Jones* that the same information, in the aggregate, becomes constitutionally cognizable. *See Jones*, 132 S. Ct at 956 (Sotomayor, J., concurring) (asking whether individuals have a reasonable expectation of privacy in the "sum of [their] public movements" or whether individuals reasonably expect that their public movements will be "recorded and aggregated in a manner that enables the Government to ascertain [a highly personal level of detail];" *id.* at 964 (Alito, J., concurring) (finding law enforcement's "catalogu[ing] every single movement of an individual's car for a very long period" constitutionally offensive). Here, the 24-hour, real-time surveillance of all of Gottesfeld's internet traffic, for 60 days, goes well beyond what ordinary people expect the government to be observing.

Alternatively, the surveillance in this case is constitutionally cognizable if viewed as the surveillance of *content* information. *See* § I.B below. The content of communications is protected

[3] Indeed, if the government is correct that its surveillance reveals that an individual visits Amazon.com, while not the particular book at Amazon.com, its surveillance reveals internet trips that are undeniably private. *Cf.*, *e.g., People v. Weaver,* 12 N.Y.3d 433, 441–442 (2009) (noting, of GPS data, that it would disclose "trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on," *quoted in Jones*, 565 U.S. at 415 (Sotomayor, J.)). The same is disclosed by cyber visits to the internet analogue to those locations.

under *Katz*, 389 U.S. 347 (legitimate expectation of privacy exists in contents of phone conversation). *See Smith*, 442 U.S. at 741 (distinguishing between the "means of establishing communication," as revealed by the pen register's recording of the phone numbers dialed, and the "purport of a[] communication," as revealed by the recording of a conversation in *Katz*); *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 135-36 (3d Cir. 2015) (discussing this distinction between "extrinsic information used to route a communication and the communicated content itself" as "loom[ing] large in federal surveillance law"). Gottesfeld contends that technology has rendered the seizure of internet "source and destination" information, Ex. B at 1, more comparable to content, under *Katz*, than to "means of establishing communication" under *Smith*. *But cf. United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008) (holding that "e-mail to/from addresses and IP addresses constitute addressing information and do not necessarily reveal any more about the underlying contents of communication than do phone numbers," while declining to "imply that more intrusive techniques or techniques that reveal more content information [would be] constitutionally identical to the use of a pen register"); *United States v. Ulbricht*, 858 F.3d 71, 97 (2d Cir. 2017).

Further supporting the conclusion that Gottesfeld had a reasonable expectation of privacy in his online activities is the fact that he used encryption services – the only way an individual can attempt to hold on to his privacy while using the internet. *See* Ex. A at ¶¶ 22-24 (stating that Gottesfeld used riseup.net, a service that provides "location anonymization and traffic encryption," and The Onion Router (TOR), "another tool used to browse the internet anonymously"); *cf. Smith v. Maryland*, 442 U.S. 735, 743 (1979) (finding that a caller's decision to use the home phone, instead of a pay phone, "was not and could not have been calculated to preserve the privacy of the number he dialed"). Where Gottesfeld was using the internet inside his own home, on his own computer, and

further encrypting his activities, he expected that his online activities were private. Society recognizes that expectation as reasonable.

2. That expectation is not forfeited simply because internet usage occurs through the service of a third party

It would be incorrect to analogize the internet information at issue here to the bank records and pen registers held not subject to Fourth Amendment protections in *Smith v. Maryland*, 442 U.S. 735 (1979), and *United States v. Miller*, 425 U.S. 435 (1976). *Smith* and *Miller* held that, by voluntarily sharing dialed numbers with the phone company and banking records with the bank, consumers waived any right to privacy in those records for purposes of the Fourth Amendment. *Smith*, 442 U.S. at 742; *Miller*, 425 U.S. at 442-43. This so-called "third party doctrine" has, until now, insulated from Fourth Amendment scrutiny the seizure of internet source and destination information from the service providers. *See Forrester*, 512 F.3d at 509-10; *Ulbricht*, 858 F.3d at 96-97. Yet the third party doctrine is at odds with the pervasive use of technology today and the concomitant expectation citizens have that the information they enter into their computers and cell phones is private. *See Jones*, 565 U.S. at 417-18 (Sotomayor, J.); *see also Riley v. California*, 134 S. Ct. 2473, 2490 (2014). For this reason, Supreme Court is poised to re-consider the third party doctrine this coming term. *See Carpenter v. United States*, S.Ct. No. 16-402 (concerning the warrantless search and seizure of records containing cell site location information).

As Justice Sotomayor recognized in *Jones*, our increasing dependence on technology in daily life requires a reevaluation of the question of "privacy" in the context of the Fourth Amendment:

> More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. *E.g., Smith,* 442 U.S. at 742, 99 S. Ct. 2577; *United States v. Miller,* 425 U.S. 435, 443, 96 S. Ct. 1619, 48 L. Ed. 2d 71 (1976). This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to

> their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers.

132 S. Ct. at 957 (Sotomayor, J., concurring); *see also* Aya Gruber, *Garbage Pails and Puppy Dog Tails: Is That What* Katz *Is Made Of?*, 41 U.C. Davis L. Rev. 781, 837 (2008) (arguing that the third-party doctrine is "extremely dangerous in an increasingly technological world" and must be reconsidered in light of actual societal expectations of privacy in digital information).

The Supreme Court has consistently revisited its Fourth Amendment jurisprudence in light of evolving technology. *See Kyllo*, 533 U.S. at 33-34 ("It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology"). *Jones* thus recognized that GPS technology was qualitatively different from its physical surveillance counterpart. 132 S. Ct. at 954. *Riley* similarly rejected any comparison between other physical items in an arrestee's possession and his cell phone. *See* 134 S. Ct. at 2485 ("A search of the information on a cell phone bears little resemblance to the type of brief physical search considered in [previously]").

Here, as in *Jones* and *Riley*, the realities of modern technology preclude the mechanical application of the 35-year-old *Smith* precedent. The Court could not have foreseen that one day the vast majority of Americans would be hooked up to the world wide web, from their homes, and accomplishing everything from banking to ordering groceries, to obtaining health information, reading news, watching TV shows, making political and charitable donations, viewing pornography, and google-mapping the earth. *See Packingham v. North Carolina*, 137 S. Ct. 1730, 1736 (U.S. 2017) ("The forces and directions of the Internet are so new, so protean, and so far reaching that courts must be conscious that what they say today might be obsolete tomorrow"). It is inconceivable that the Supreme Court in *Smith* and *Miller* intended so far-reaching an abrogation of our Fourth Amendment rights. *See United States v. Cooper*, No. 13-CR-00693-SI-1, 2015 WL 881578, at *6 (N.D.

Cal. Mar. 2, 2015)("[T]he pen registers employed in 1979 bear little resemblance to their modern day counterparts").

More and more states are rejecting or curtailing *Smith* and recognizing a reasonable expectation of privacy in information revealed to technology companies. *See, e.g., Commonwealth v. Augustine*, 4 N.E.3d 846, 861-62 (Mass. 2014) (rejecting *Smith* and finding reasonable expectation of privacy in cell site location information under state constitution); *State v. Earls*, 70 A.3d 630, 644 (N.J. 2013) (reasonable expectation of privacy in cell site location information); *Tracey v. State* 152 So. 3d 504, 525 (Fla. 2014) (same); 86 Ops. Cal. Atty. Gen. 198 at *3-4 (2003) (information obtained from pen/trap devices protected under state constitution). This is as it should be and as it eventually must be in the federal system. The "Cyber Age is a revolution of historic proportions." *Packingham*, 137 S. Ct. at 1736. It cannot be permitted to "erode the privacy guaranteed by the Fourth Amendment." *Kyllo*, 533 U.S. at 34.

B. THE SURVEILLANCE EXCEEDED STATUTORY AUTHORITY BECAUSE IT REVEALED CONTENT INFORMATION

18 U.S.C. § 3122(a)(1) permits the government to apply for "...an order under section 3123 of this title authorizing or approving the installation and use of a pen register or a trap and trace device." Pen register/trap and trace ("pen/trap") is a "device or process" which "records," "decodes," or "captures" the "dialing, routing, addressing, or signaling information" on outgoing communications or "the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing and signaling information reasonably likely to identify the source of a wire or electronic communication." 18 U.S.C. § 3127(3)&(4). "[S]uch information shall not include the contents of any communication." 18 U.S.C. § 3127(3)&(4); *see also In re Application of U.S. for an Order Authorizing use of A Pen Register & Trap On (XXX) Internet Serv. Account/User Name, (xxxxxxxx@xxx.com),* 396 F. Supp. 2d 45, 47 (D. Mass. 2005) ("[T]he government is not entitled to receive '...dialing, routing, addressing, or signaling information …

reasonably likely to identify the source of a wire or electronic communication" … if [that information]… reveals the 'contents' of a communication"); *United States v. Willard,* No. 3:10-CR-154, 2010 WL 3784944, at *2 (E.D. Va. Sept. 20, 2010) ("When using a pen register or trap and trace device on a computer, the government is not entitled to receive information from the device if that information reveals the contents of a communication"). "'[C]ontents', when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport or meaning of that communication." 18 U.S.C. § 2510(8).

Gottesfeld contends that a continuous tracking of his online activities, in real time, 24 hours a day for 60 days, garners information that constitutes "content." Whereas in the times of telephones, the distinction between numbers dialed and the "content" of a conversation was clear, that line has been blurred by our vast and expanding use of technology. *See In re Application*, 396 F. Supp. 2d at 47-48 (noting the difficulty and considering bank account numbers and search terms to be types of content); *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 138 (3d Cir. 2015) ("under the surveillance laws, 'dialing, routing, addressing, and signaling information' may also be 'content'").

The government, in its application, offers this line of demarcation: "the website 'Amazon.com' does not contain the content of any communication, a URL that lists what book the user is searching for on Amazon.com could be considered to contain the content of a communication." Ex. B at 4 n.2; *see also Forrester*, 512 F.3d at 504 n.6 (drawing the same distinction: "a surveillance technique that captures IP addresses would show only that a person visited the New York Times' website at http://www.nytimes.com, whereas a technique that captures URLs would also divulge the particular articles the person viewed").

Yet there is no principled distinction between the two; "content" is a matter of degree. *See Forrester*, 512 F.3d at 510 n. 6 ("[a] URL, unlike an IP address, identifies the particular document

within a website that a person views and thus reveals *much more* information about the person's [i]nternet activity" (emphasis added)). Government surveillance that reveals that a citizen, in his own home, views The New York Times, Amazon.com, WebMd – or Pornhub – reveals a trove of information about his life. That more detailed search information – which book, which kind of pornography – would reveal *more* content does not render the destination information, in the aggregate, mere "means of establishing communication." *Smith*, 442 U.S. at 741; *see Jones*, 132 S. Ct at 956 (Sotomayor, J., concurring) (noting that "the sum of" data points which are innocuous and public, on an atomized level, become meaningful and private when viewed in the aggregate). *But cf. Ulbricht*, 858 F.3d at 96 (affirming the warrantless collection of "IP address information devoid of content"); *Forrester*, 512 F.3d at 510 ("e-mail to/from addresses and IP addresses …do not necessarily reveal any more about the underlying contents of communication than do phone numbers").

Moreover, the government here has obtained a layer of information beyond simply the IP addresses with whom Gottesfeld communicated. The warrant application avers that Gottesfeld used the VPN network at riseup.net, *see* Ex. A at ¶ 22, and the TOR network, *id.* ¶ 24. Yet the government would have no way to know, from the IP addresses alone, that he was using that particular service at that IP address. It must have received additional routing information, therefore.

Nor do the government's statements, in the application and proposed order, that it "does not seek the URL for websites visited by the designated account, as this URL could contain content," Ex. B at 1, 4, adequately ensure that the service provider did not simply turn over all of the information, rather than sifting through to discard any content-revealing information. More is required:

> [A] mere statement in an order authorizing the installation of a pen register and/or a trap and trace device that the internet service provider is to disclose only "dialing, routing, addressing and signaling information" and not to reveal "contents" and, in addition, not to

> disclose "dialing, routing, addressing and signaling information" which contains "contents" is insufficient notice to the internet service provider as to what may and may not be disclosed. Accordingly, in my judgment, an order to an internet service provider should contain a listing, to the extent possible, of what may NOT be disclosed pursuant to the order.

In re Application, 396 F. Supp. 2d at 49 (D. Mass. 2005).

No such safeguards were provided here. *See id.* ("to impose upon the internet service providers the necessity of making sure that they configure their software in such a manner as to disclose only that which has been authorized, the Court will include a provision to the effect that a violation of the order, including the disclosure of prohibited information, may be found to be a contempt of Court and subject the violator to punishment); *see also In Matter of Application of U.S. For an Order Authorizing the Installation & Use of a Pen Register & a Trap & Trace Device on E-Mail Account,* 416 F. Supp. 2d 13, 18 (D.D.C. 2006) (noting that "some caution… is warranted to make certain the court order clearly identifies what is permitted and, more importantly, what is prohibited so there is no question about the scope of the authorized activities," and finding this caution was exercised when the application and proposed order "explicitly identif[ied] the information the process or device [wa]s intended to collect and noticeably omit[ted] content from the request").

Suppression should be the remedy for a violation of the pen/trap statute. It is the only avenue available to vindicate the rights at issue. *See Hudson v. Michigan*, 547 U.S. 586, 126 S.Ct. 2159, 2163, 165 L.Ed.2d 56 (2006) ("Suppression of evidence ...has always been our last resort"). *But cf. United States v. Fregoso*, 60 F.3d 1314, 1320 (8th Cir.1995) ("[T]he statutory scheme [of the pen register statute] does not mandate exclusion of evidence for violations of the statutory requirements."); *United States v. Thompson*, 936 F.2d 1249, 1249–50 (11th Cir.1991).

C. THE SURVEILLANCE VIOLATED THE STORED COMMUNICATIONS ACT BECAUSE THE GOVERNMENT DID NOT SHOW ARTICULABLE FACTS

The Stored Communications Act, 18 U.S.C. § 2703(d), permits courts to order a third-party communications provider to turn over records when the government "offers specific and articulable facts showing that there are reasonable grounds to believe that" the records sought "are relevant and material to an ongoing criminal investigation." *Id.* Here, the government failed to provide "specific and articulable facts" suggesting that Gottesfeld's internet traffic from three months after the DDOS attack would be relevant, in any way, to its investigation.[4] To the contrary. The application states that the DDOS attack happened. Ex. B. at ¶ 15. Records for the account that posted the Youtube video directed towards Boston Children's Hospital gave an IP address to which Gottesfeld was linked. *Id.* at ¶¶ 16-17. From those two pieces of information, the government concludes that "a computer, tablet, smartphone, or other internet-enabled device" at Gottesfeld's house was used to post the Youtube video. *Id.* at ¶ 18. This fails entirely to suggest any relevance for surveillance of Gottesfeld's internet traffic from July to September of 2014. *See* Ex. B at 5 (requesting real-time information for his online activities "continuously, 24 hours per day," on July 17, 2014). Thus, the order violates the Stored Communications Act. For the reasons stated above, suppression is an appropriate remedy.

D. THE REAL-TIME COLLECTION OF CONTENT INFORMATION VIOLATED THE WIRETAP ACT

In order to intercept the *content* of any electronic communication, the government needs a wiretap order. *See In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 136 & nn.31-32 (3d Cir. 2015) (explaining that "Whereas the Wiretap Act governs the interception of communications 'content[ ],' the separate federal Pen Register Act governs the acquisition of non-

[4] The attack took place on April 20, 2014. The government requested 60 days of surveillance beginning July 17, 2014.

content 'dialing, routing, addressing, [or] signaling information.'"); 18 U.S.C. § 2510(4) (defining "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device"). To obtain a wiretap order, the government must show probable cause and necessity. *See* § 2518(1)(c); *United States v. Williams*, 524 F. App'x 195, 200 (6th Cir. 2013).

Because the information the government obtained in this case was content information, rather than purely "means of communication," *see In re* Google, 806 F.3d at 136, its real-time surveillance of Gottesfeld violated the Wiretap Act. The evidence should be suppressed on this basis as well.

II. ABSENT THE ILLEGALLY OBTAINED INFORMATION, THE WARRANT CANNOT STAND

The information contained in the search warrant affidavit that was obtained in violation of Gottesfeld's Fourth Amendment rights, namely ¶¶21-26, must be excised from the affidavit for purposes of determining whether probable cause existed to justify issuance of the warrant. *See United States v. Asaro*, 2014 U.S. Dist. LEXIS 84171, *9, No. 12-10196-GAO (D. Mass. June 20, 2014) (writing that when evidence that was obtained in violation of constitutional rights is included in warrant application, suppression is warranted "only if, the 'offending information' being ignored, what remained in the affidavit was insufficient to establish probable cause") (citing *United States v. Dessesaure*, 429 F.3d 359, 367 (1st Cir. 2005); *accord United States v. Zhen Zhou Wu*, 2010 U.S. Dist. LEXIS 4439 (D. Mass. Jan. 21, 2010)). In this particular case, the Court should excise from the affidavit the fact that Gottesfeld used a VPN service through the website www.riseup.net, as well as the fact that he used the TOR network, both services used by individuals seeking to browse the internet anonymously.

Putting aside the unlawfully obtained information about Gottesfeld's internet activity, the affidavit fails to establish probable cause that evidence of a crime would be found at that location. The government had evidence that Gottesfeld was the one who posted the Anonymous video on YouTube almost a month before the DDOS attack on Children's Hospital. However, they have no information about where the DDOS attack came from. In fact, they admit as such in their search warrant application: "I have reviewed BCH webserver logs from the time of the DDOS attack. These logs showed hundreds of IP addresses flooding the BCH network with malicious traffic. The IP addresses sending this malicious traffic resolve to geographically dispersed locations." Ex. A. at ¶15.

Without the information regarding Gottesfeld's use of riseup.net's VPN service and the TOR network, the affiant would not be able to give his opinion that these services are often used by criminals "in an effort to evade law enforcement." Ex. A. at ¶26. The affiant also would not be able to link Gottesfeld in any way to two Twitter accounts, @AnonMercurial and @PacketSignal, which tweeted about the Children's Hospital DDOS attack using TOR and riseup.net IP addresses. *Id.* at ¶25.

What the government is left with when the internet traffic information is excised is that Gottesfeld posted the YouTube video about a month before the attack, as well as that Gottesfeld is an activist against the "troubled teen industry" and had been outspoken against two other organizations that experienced DDOS attacks. Ex. A. at ¶¶27-31. Those facts, however, do not establish probable cause to believe that Gottesfeld committed those DDOS attacks, or that evidence of any crime would be found at his apartment.

III. THE SEARCH WARRANT IS UNCONSTITUTIONALLY OVERBROAD

Given the pervasive and personal nature of technology, warrants must be tailored to seize only those devices that are (a) connected to the person being targeted and (b) connected to the

crime. Here, the warrant gave the government blanket permission to seize "[a]ll computer hardware," and "any computer hardware (including smartphones and tablets), computer software, or storage media …." Attachment B (Items to be Seized) to Search Warrant (here, Ex. A) at ¶ I.D, ¶ II. It is in no way tailored to the type of device suspected – or even capable – of causing the DDOS attack. Furthermore, the warrant goes beyond seizing devices of Gottesfeld's. It gives the government permission to seize literally "any" computer, phone, tablet, "or storage media" that is at the house. Indeed, the affidavit affirmatively *requests* permission to "search and seize… on-site or off-site …, regardless of how their contents or ownership appear or are described by others at the scene of the search." Ex. A ¶ 35. It fails to justify why it needs unfettered access to *anyone*'s devices, *of any kind*, that may happen to be at that address on that day. Such a warrant has been held to be unconstitutionally overbroad. *See United States v. Griffith*, No. 13-3061, 2017 WL 3568288, at *7 (D.C. Cir. Aug. 18, 2017) (finding search warrant for the seizure "of all electronic devices found in the residence," a year after a gang-related homicide, was unconstitutionally overbroad). Furthermore, the warrant granted permission not only to seize the items, but to search them as well. *See United States v. Cotterman*, 709 F.3d 952, 964 (9th Cir. 2013) (en banc) (noting the "private information individuals store on digital devices—their personal 'papers' in the words of the Constitution"); *cf. Griffith*, No. 13-3061, 2017 WL 3568288, at *16 (Brown, J., dissenting) (noting that the warrant in that case "only authorized the *seizure* of the electronic devices, not a *search* of their content" (emphasis in original). Because the search warrants fails to describe with any particularity the things to be seized, the warrant issued in violation of the Fourth Amendment's requirement that warrants "particularly describ[e]" the "things to be seized." The warrant is therefore invalid and evidence obtained pursuant to the execution of this warrant must be suppressed.

CONCLUSION

For the reasons set forth above, the search warrant in this case cannot stand. The Court should suppress any items seized from the house and any information obtained as a result of those items.

MARTIN GOTTESFELD,
By His Attorneys,

/s/ Jane F. Peachy
Jane F. Peachy, BBO#661394

/s/ Amy Barsky
Cal. Bar 270846

Federal Defender Office
51 Sleeper Street, 5th Floor
Boston, MA 02210
Tel: 617-223-8061

CERTIFICATE OF SERVICE

I, Jane F. Peachy, Esquire, hereby certify that this document filed through the ECF system will be sent electronically to the registered participant(s) as identified on the Notice of Electronic Filing (NEF) on August 31, 2017.

/s/ Jane F. Peachy
Jane F. Peachy